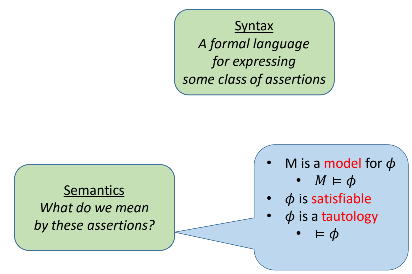
Review
Program Verification => Satisfiability

```
method Eg1 (x, y, z: bool)
{
   var result : bool;
   if (x)
      result := y;
   else
      result := z;
   assert result;
}
```

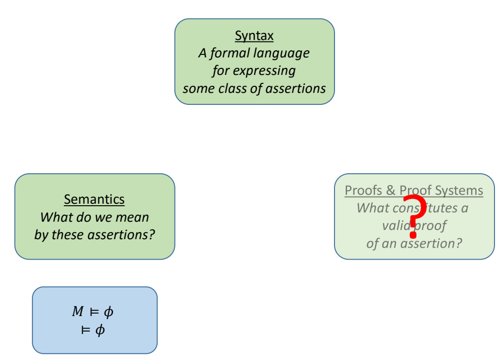
(x, y, z) is a counterexample iff $(\neg x \vee \neg y) \wedge (x \vee \neg z)$

Review
Propositional Logic



Propositional Satisfiability

- How can we check if
  - ϕ is a tautology?
  - ϕ is satisfiable?
- Decidable
  - Only finitely many cases to check
  - (Finite-state) model checking
- Efficiency?
  - Original NP-Complete problem
  - But very good SAT solvers have been developed over the years …



Formal Proofs & Proof Systems

- Exhaustive checking does not work, e.g., when we reason about integers:
  - For all x, y, z, $(x < y) \wedge (z = \frac{x+y}{2}) \Rightarrow (z < y)$
- Need other approaches to proofs
- Goal: Finite reasoning about infinitely many possibilities

First Order Logic
aka
Predicate Calculus

Propositional Logic +

- Variables: $x, y, z, \ldots$
- Function symbols: $f, g, +, \times, \cdot$
  - arity: number of operands
  - prefix notation: $f(x, y)$
  - infix notation: $x + y$
  - constant symbols: $0, 1, \ldots$
- Predicate symbols: $p, q, >, \geq$
  - Equality predicate: $x = y$ (Predefined "predicate" with a fixed meaning/interpretation)
- Quantification (Universal/Existential)

Examples

- Natural numbers (Peano arithmetic)
  - Constant symbol: 0
  - Function symbol: S (successor function)
- Natural numbers:
  - Constant symbol: 0
  - Function symbol: S (successor function)
  - Function symbols: $+, \times$
- Set theory
  - Constant symbol: ϕ (optional)
  - Predicate symbol: $\in$

First Order Logic: Syntax

- The set of terms:

$$\tau \ ::= \ f(\tau_1 \cdots, \tau_n) \ | \ x$$

- The set of formula:

$$\phi \ ::= p(\tau_1, \cdots, \tau_n) \ | \ \tau_1 = \tau_2 \ |$$
$$\neg\phi \ | \ \phi_1 \wedge \phi_2 \ | \ \phi_1 \vee \phi_2 \ | \forall x. \phi \ | \ \exists x. \phi$$

First Order Logic
Semantics (informally)

- Consider natural numbers $(0, S, +, \times)$
- Encode "x is less than or equal to y"
  - $\exists z. y = x + z$
- Consider sets $(\in)$
- Encode "x is a subset of y"
  - $\forall z.\ z \in x \ \Rightarrow \ z \in y$
- Encode "z is the union of x and y"
  - $\forall w. (w \in x) \ \Leftrightarrow \ (w \in x) \vee (w \in y)$

First Order Logic
Semantics (informally)

- Understanding quantification …
  - $\forall x. \exists y. (x < y)$
  - $\exists y. \forall x. (x < y)$
- Conversions between $\exists$ and $\forall$
  - $\neg\exists x. \phi(x)$ equivalent to $\forall x. \neg\phi(x)$
  - $\neg\forall x. \phi(x)$ equivalent to $\exists x. \neg\phi(x)$

First Order Logic
Semantics (informally)

- What do the following mean?
  a) $\exists x \ \forall y \ x \oplus y = y$
  b) $\exists x \ \forall y \ (x \oplus y = y) \wedge (y \oplus x = y)$
  c) $\forall x \ \forall y \ x \oplus y = y \oplus x$
- Does (a) hold
  - If we consider the set of integers and interpret $\oplus$ as integer-addition?
- Find an example of a set and an operation $\oplus$ that does not satisfy (a)

First Order Logic: Semantics

- We can interpret terms and formulae …
- … given the *meaning* of the function symbols and predicate symbols
  - A set A (the universe)
  - For every function-symbol f of arity n, a function $M[f] : A^n \rightarrow A$ representing the interpretation of f
  - For every predicate-symbol p of arity n, a function $M[p]: A^n \rightarrow \{T, F\}$ representing the interpretation of p
  - (called a *structure* or *interpretation* for the underlying language)
  - We will refer to the structure as M

First Order Logic: Semantics

- Extend the interpretation-function to define the value $M[\tau] \in A$ for any term τ inductively.
- We write $M \vDash \phi$ to denote that ϕ holds true in the interpretation M.
- We define $M \vDash \phi$ inductively.

Mathematical Preliminaries

Inductive Definitions

- Syntax $\qquad \phi ::= P \;\mid\; \phi_1 \vee \phi_2 \;\mid\; \phi_1 \wedge \phi_2$
- Semantics
- Proof rules

$$\frac{M[\phi_1] = T, \qquad M[\phi_2] = T}{M[\phi_1 \wedge \phi_2] = T}$$

- Type systems

$$\frac{M \vdash \phi_1, \qquad M \vdash \phi_2}{M \vdash \phi_1 \wedge \phi_2}$$

Example

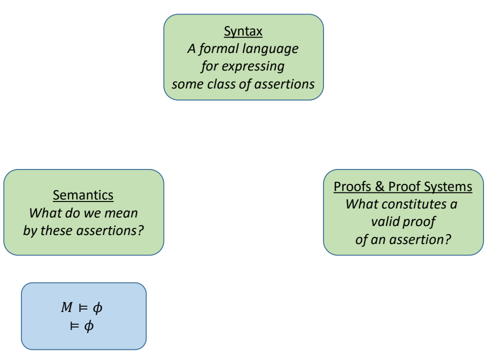
- Consider the language with
  - function symbols $\oplus$ and $\otimes$ of arity 2, and
  - function (constant) symbols c_0 and c_1 of arity 0
- Let M denote the following structure
  - The universe is the set of integers
  - $M[\oplus]$ is integer-addition
  - $M[\otimes]$ is integer-multiplication
  - $M[c_0]$ is 0
  - $M[c_1]$ is 1

Example

- Does $M \vDash \neg\exists x.(x \otimes x) \oplus c_1 = c_0$ hold?
- Is there any structure N such that
  $N \vDash \exists x.(x \otimes x) \oplus c_1 = c_0$

Semantic Concepts

- M is said to be a model for ϕ iff $M \vDash \phi$
- We say M is a model of a set $\{\psi_1, \psi_2, \cdots\}$ if M is a model of every ψ_i in the set
- ϕ is said to be satisfiable if it has a model
- ϕ is said to be unsatisfiable if it has no model
- ϕ is said to be valid (or a tautology) if every interpretation M is a model for ϕ
- We write $\vDash \phi$ iff ϕ is a tautology



Axiomatic Reasoning

- Consider the language (of group theory)
  - one nullary function symbol e
  - one unary function symbol I
  - one binary function symbol $\oplus$
- Consider the following "axioms":
  - A_1: $\forall x \forall y \forall z. x \oplus (y \oplus z) = (x \oplus y) \oplus z$
  - A_2: $\forall x. e \oplus x = x$
  - A_3: $\forall x. I(x) \oplus x = e$
  - A_2': $\forall x. x \oplus e = x = x$
  - $A_3{}'$: $\forall x. x \oplus I(x) = e$

Example

- Let ϕ denote the formula
  $\forall x\, \forall y\, \forall z. (x \oplus y = x \oplus z) \Rightarrow y = z$
- What does ϕ say?
- Let M be a structure such that
  - $M \vDash A_1$
  - $M \vDash A_2$
  - $M \vDash A_3$
- Does $M \vDash \phi$ hold?

Axiomatization

- We write $\{A_1, A_2, A_3\} \vDash \varphi$ to mean that
  - Every model of $\{A_1, A_2, A_3\}$ is a model of φ
  - I.e., if M is any structure such that $M \vDash A_1$, and $M \vDash A_2$ and $M \vDash A_3$ then $M \vDash \varphi$.
- Let Ψ be a set of formula (axioms or axiom schemas)
- We write $\Psi \vDash \varphi$ to mean that
  - Every model of Ψ is a model of φ
  - Thus, $\varphi$is a semantic consequence of Ψ
  - A semantic concept … no easy way to check.
- The theory of Ψ is the set of all φ such that $\Psi \vDash \varphi$

Axiomatization

- Suppose we "axiomatize" M using a set Ψ of formula (axioms)
  - That is, $M \vDash \psi$ for every $\psi \in \Psi$
  - That is, M is a model of Ψ
- Problem reduction:

Does $M \vDash \phi$? $\overset{\Leftarrow}{\underset{\Rightarrow ?}{\longrightarrow}}$ Does $\Psi \vDash \phi$?

Theory Completeness

- For every φ (with no free variables)
  - Either $M \vDash \varphi$ or $M \vDash \neg\varphi$
  - It is possible that neither $\Psi \vDash \varphi$ nor $\Psi \vDash \neg\varphi$
- We say that Ψ is complete (or the theory of Ψ is complete) if
  - for every φ either $\Psi \vDash \varphi$ or $\Psi \vDash \neg\varphi$